(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 188 445 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
05.07.2017 Bulletin 2017/27

(21) Application number: **14902723.7**

(22) Date of filing: **31.10.2014**

(51) Int Cl.:
H04L 29/08 *(2006.01)*

(86) International application number:
PCT/CN2014/090092

(87) International publication number:
WO 2016/045167 (31.03.2016 Gazette 2016/13)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **26.09.2014 CN 201410505903**

(71) Applicant: **Yulong Computer Telecommunication Scientific (Shenzhen) Co., Ltd.**
Shenzhen, Guangdong 518057 (CN)

(72) Inventor: **LUO, Limin**
Shenzhen
Guangdong 518040 (CN)

(74) Representative: **Johnson, Richard Alan et al**
Mewburn Ellis LLP
City Tower
40 Basinghall Street
London EC2V 5DE (GB)

(54) DATA TRANSMISSION METHOD, APPARATUS, AND SYSTEM

(57) The present disclosure provides a data transmission method which is applied in a terminal. The terminal includes multiple operating systems, wherein each operating system corresponds to a transmission module. The method includes: determining a target transmission mode for data of the terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode includes a normal transmission mode and a secure transmission mode; switching from the current operating system of the terminal to a designated operating system of the multiple operating systems when the target transmission mode is the secure transmission mode, and establishing a connection with the target terminal via the designated operating system; determining whether the target terminal supports secure transmission; transmitting the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission. Correspondingly, the present disclosure further provides a data transmission device and a data transmission system. By means of the technical solution of the present disclosure, secure transmission and storage of user secure data can be ensured, and malicious attacks from other operating systems can be avoided.

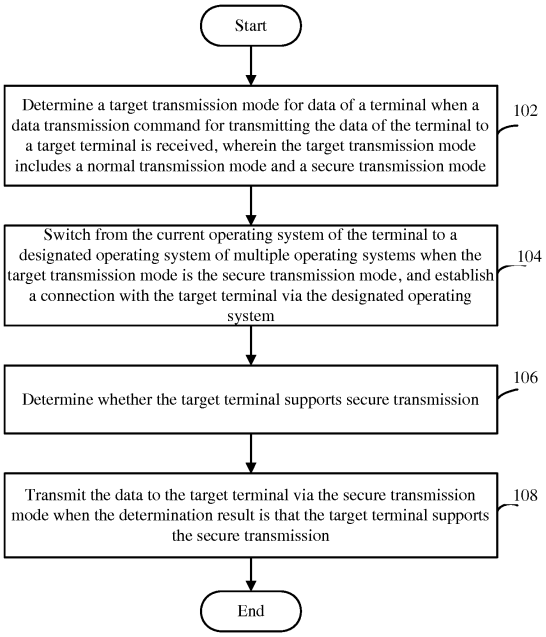

FIG. 1

EP 3 188 445 A1

Description

TECHNICAL FIELD

[0001] The present disclosure relates to the technical field of terminals, and in particular, to a data transmission method, a data transmission device, and a data transmission system.

BACKGROUND

[0002] Presently, when mobile phone terminals share data, a connection is directly established between a transmitter and a receiver, and the transmitter directly transmits data to the receiver. The transmitter cannot determine whether the reception environment of the receiver is secure, which may result in a risk of stealing and eavesdropping after content is received.

[0003] Therefore, what is needed is a new technical solution, which can ensure security of shared data when the transmitter and the receiver share data, and prevent the problem that the shared data is stolen or eavesdropped after the receiver receives the shared data.

SUMMARY

[0004] Based on the above problems, the present disclosure provides a new technical solution, which can ensure security of shared data when a transmitter and a receiver share data, and prevent the problem that the shared data is stolen or eavesdropped after the receiver receives the shared data.

[0005] In view of the above, the present disclosure provides a data transmission method which is applied in a terminal. The terminal includes multiple operating systems, wherein each operating system corresponds to a transmission module. The method includes: determining a target transmission mode for data of the terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode includes a normal transmission mode and a secure transmission mode; switching from the current operating system of the terminal to a designated operating system of the multiple operating systems when the target transmission mode is the secure transmission mode, and establishing a connection with the target terminal via the designated operating system; determining whether the target terminal supports secure transmission; transmitting the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission.

[0006] In the technical solution, when a user of the terminal wants the data to be securely transmitted, the secure transmission mode can be selected. When the terminal detects that the transmission mode for the data is the secure transmission, and the current operating system is not the designated operating system, the user is prompted to switch to the designated operating system or the terminal automatically switches to the designated operating system. Specifically, the designated operating system can be a secure operating system. A connection with the target terminal of the receiver is then established, and whether the target terminal supports the secure transmission is determined, that is, whether the target terminal includes a secure operating system or a secure transmission module is determined. When the determination result is yes, the data is transmitted to the target terminal via the secure transmission mode, thereby ensuring data security during data transmission and after the data is transmitted to the target terminal.

[0007] In the above technical solution, preferably, the method further includes prompting the user of the terminal to terminate the transmission of the data or adopt the normal transmission mode to transmit the data to the target terminal when the determination result is that the target terminal does not support the secure transmission.

[0008] In the technical solution, when the target terminal does not support the secure transmission, for ensuring security of transmission of the data, the user is prompted to terminate the transmission of the data, or to adopt the normal transmission mode to directly transmit the data.

[0009] In the above technical solution, preferably, determining whether the target terminal supports the secure transmission includes: sending a transmission environment check command to the target terminal, so as to cause the target terminal to check whether a corresponding designated operating system is included according to the transmission environment check command, and send a support response to the terminal when the determination result is yes; and determining whether the support response is received from the target terminal, determining that the target terminal supports the secure transmission when the determination result is yes, and determining that the target terminal does not support the secure transmission when the determination result is no.

[0010] In the technical solution, the terminal of the transmitter sends the transmission environment check command to the target terminal of the receiver, and the target terminal determines whether the designated operating system is included according to the command, that is, whether the secure operating system is included. The target terminal sends the support response when the designated operating system is included, so as to inform the terminal of the transmitter that the secure transmission can be performed.

[0011] In the above technical solution, preferably, transmitting the data to the target terminal via the secure transmission mode includes: establishing a connection between a first transmission module corresponding to the designated operating system of the terminal and a second transmission module corresponding to the designated operating system of the target terminal, and transmitting the data from the first transmission module to the second transmission module.

[0012] In the technical solution, when the data can be transmitted via the secure transmission mode, it indicates that the terminal of the transmitter has the designated operating system and the transmission module corresponding to the designated operating system, and the terminal of the receiver has the designated operating system and the transmission module corresponding to the designated operating system. At this point, a transmission channel is established between the two transmission modules, thereby ensuring security of transmission of the data.

[0013] Specifically, data transmission can be directly performed between the designated operating system for example the secure operating system and a designated operating system of the other terminal, for example, data is directly transmitted from a secure operating system of a terminal A to a secure operating system of a terminal B.

[0014] Furthermore, for ensuring security of the data of the terminal, the secure operating system may not be allowed to directly communicate with external devices to perform data service. At this point, when data transmission is performed, the data of the secure operating system can be transmitted to the other normal operating system of the terminal, and the data is then transmitted from the other normal operating system of the terminal to a normal operating system of an external target terminal, and then the data is transmitted from the normal operating system to a designated operating system, that is, a secure operating system.

[0015] For further ensuring security of data, encryption processing can be performed on transmission of the data. After the target terminal of the receiver receives the data, decryption processing is performed.

[0016] In the above technical solution, preferably, the designated operating system is the operating system of the multiple operating systems having the highest security level.

[0017] In the technical solution, the operating system having the highest security level, that is, the secure operating system is set to be the designated operating system, thus the security of data transmission and data storage can be ensured.

[0018] According to another aspect of the present disclosure, a data transmission device is further provided. The data transmission device is applied in a terminal. The terminal includes multiple operating systems, wherein each operating system corresponds to a transmission module. The data transmission device includes: a determining unit configured to determine a target transmission mode for data of the terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode includes a normal transmission mode and a secure transmission mode. The device further includes a connection establishing unit configured to switch from the current operating system of the terminal to a designated operating system of the multiple operating systems when the target transmission mode is the secure transmission mode, and establish a connection with the target terminal via the designated operating system, a judging unit configured to determine whether the target terminal supports secure transmission, and a transmitting unit configured to transmit the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission.

[0019] In the technical solution, when a user of the terminal wants the data to be securely transmitted, the secure transmission mode can be selected. When the terminal detects that the transmission mode for the data is the secure transmission, and the current operating system is not the designated operating system, the user is prompted to switch to the designated operating system or the terminal automatically switches to the designated operating system. Specifically, the designated operating system can be a secure operating system. A connection with the target terminal of the receiver is then established, and whether the target terminal supports the secure transmission is determined, that is, whether the target terminal includes a secure operating system or a secure transmission module is determined. When the determination result is yes, the data is transmitted to the target terminal via the secure transmission mode, thereby ensuring data security during data transmission and after the data is transmitted to the target terminal.

[0020] In the above technical solution, preferably, the device further includes a prompting unit configured to prompt the user of the terminal to terminate the transmission of the data or adopt the normal transmission mode to transmit the data to the target terminal when the determination result is that the target terminal does not support the secure transmission.

[0021] In the technical solution, when the target terminal does not support the secure transmission, for ensuring security of transmission of the data, the user is prompted to terminate the transmission of the data, or to adopt the normal transmission mode to directly transmit the data.

[0022] In the above technical solution, preferably, the judging unit includes a sending unit configured to send a transmission environment check command to the target terminal, so as to cause the target terminal to check whether a corresponding designated operating system is included according to the transmission environment check command, and send a support response to the terminal when the determination result is yes, and a deciding unit configured to determine whether the support response is received from the target terminal, determine that the target terminal supports the secure transmission when the determination result is yes, and determine that the target terminal does not support the secure transmission when the determination result is no.

[0023] In the technical solution, the terminal of the transmitter sends the transmission environment check command to the target terminal of the receiver, and the target terminal determines whether the designated op-

erating system is included according to the command, that is, whether the secure operating system is included. The target terminal also sends the support response when the designated operating system is included, so as to inform the terminal of the transmitter that secure transmission can be performed.

[0024] In the above technical solution, preferably, the transmitting unit is configured to establish a connection between a first transmission module corresponding to the designated operating system of the terminal and a second transmission module corresponding to the designated operating system of the target terminal, and transmit the data from the first transmission module to the second transmission module.

[0025] In the technical solution, when the data can be transmitted via the secure transmission mode, it indicates that the terminal of the transmitter has the designated operating system and the transmission module corresponding to the designated operating system, and the terminal of the receiver has the designated operating system and the transmission module corresponding to the designated operating system. At this point, a transmission channel is established between the two transmission modules, thereby ensuring security of transmission of the data.

[0026] Specifically, data transmission can be directly performed between the designated operating system for example the secure operating system and a designated operating system of the other terminal, for example, data is directly transmitted from a secure operating system of a terminal A to a secure operating system of a terminal B.

[0027] Furthermore, for ensuring security of the data of the terminal, the secure operating system may not be allowed to directly communicate with external devices to perform data service. At this point, when data transmission is performed, the data of the secure operating system can be transmitted to the other normal operating system of the terminal, and the data is then transmitted from the other normal operating system of the terminal to a normal operating system of an external target terminal, and then the data is transmitted from the normal operating system to a designated operating system, that is, a secure operating system.

[0028] For further ensuring security of the data, encryption processing can be performed on transmission of the data. After the target terminal of the receiver receives the data, decryption processing is performed.

[0029] In the above technical solution, preferably, the designated operating system is the operating system of the multiple operating systems having the highest security level.

[0030] In the technical solution, the operating system having the highest security level, that is, the secure operating system is set to be the designated operating system, thus the security of data transmission and data storage can be ensured.

[0031] According to yet another embodiment of the present disclosure, a data transmission system is further provided, and the data transmission system includes the data transmission device of any of the above technical solutions.

[0032] By means of the above technical solution, secure transmission and storage of user secure data can be ensured, and malicious attacks from other operating systems can be avoided.

BRIEF DESCRIPTION OF DRAWINGS

[0033]

FIG. 1 is a flow chart of a data transmission method in accordance with an embodiment of the present disclosure.

FIG. 2 is a block diagram of a data transmission device in accordance with an embodiment of the present disclosure.

FIG. 3 is a diagrammatic view of a data transmission system in accordance with an embodiment of the present disclosure.

FIG. 4 is a detailed flow chart of a data transmission method in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0034] To understand the above-mentioned purposes, features and advantages of the present disclosure more clearly, the present disclosure will be further described in detail below in combination with the accompanying drawings and the specific implementations. It should be noted that, the embodiments of the present application and the features in the embodiments may be combined with one another without conflicts.

[0035] Many specific details will be described below for sufficiently understanding the present disclosure. However, the present disclosure may also be implemented by adopting other manners different from those described herein. Accordingly, the protection scope of the present disclosure is not limited by the specific embodiments disclosed below.

[0036] FIG. 1 is a flow chart of a data transmission method in accordance with an embodiment of the present disclosure.

[0037] As illustrated by FIG. 1, a data transmission method in accordance with an embodiment of the present disclosure includes: step 102, determining a target transmission mode for data of a terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode includes a normal transmission mode and a secure transmission mode; step 104, switching from the current operating system of the terminal to a designated operating system of multiple operating systems when the target transmission mode is the secure transmission mode, and establishing a connection with the target terminal via the designated operating system; step

106, determining whether the target terminal supports secure transmission; step 108, transmitting the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission.

[0038] In the technical solution, when a user of the terminal wants the data to be securely transmitted, the secure transmission mode can be selected. When the terminal detects that the transmission mode for the data is the secure transmission, and the current operating system is not the designated operating system, the user is prompted to switch to the designated operating system or the terminal automatically switches to the designated operating system. Specifically, the designated operating system can be a secure operating system. A connection with the target terminal of the receiver is then established, and whether the target terminal supports the secure transmission is determined, that is, whether the target terminal includes a secure operating system or a secure transmission module is determined. When the determination result is yes, the data is transmitted to the target terminal via the secure transmission mode, thereby ensuring data security during data transmission and after the data is transmitted to the target terminal.

[0039] In the above technical solution, preferably, the method further includes prompting the user of the terminal to terminate the transmission of the data or adopt the normal transmission mode to transmit the data to the target terminal when the determination result is that the target terminal does not support the secure transmission.

[0040] In the technical solution, when the target terminal does not support the secure transmission, for ensuring security of transmission of the data, the user is prompted to terminate the transmission of the data, or to adopt the normal transmission mode to directly transmit the data.

[0041] In the above technical solution, preferably, determining whether the target terminal supports the secure transmission includes: sending a transmission environment check command to the target terminal, so as to cause the target terminal to check whether a corresponding designated operating system is included according to the transmission environment check command, and send a support response to the terminal when the determination result is yes; and determining whether the support response is received from the target terminal, determining that the target terminal supports the secure transmission when the determination result is yes, and determining that the target terminal does not support the secure transmission when the determination result is no.

[0042] In the technical solution, the terminal of the transmitter sends the transmission environment check command to the target terminal of the receiver, and the target terminal determines whether the designated operating system is included according to the command, that is, whether the secure operating system is included. The target terminal sends the support response when the designated operating system is included, so as to inform the terminal of the transmitter that the secure transmission can be performed.

[0043] In the above technical solution, preferably, transmitting the data to the target terminal via the secure transmission mode includes: establishing a connection between a first transmission module corresponding to the designated operating system of the terminal and a second transmission module corresponding to the designated operating system of the target terminal, and transmitting the data from the first transmission module to the second transmission module.

[0044] In the technical solution, when the data can be transmitted via the secure transmission mode, it indicates that the terminal of the transmitter has the designated operating system and the transmission module corresponding to the designated operating system, and the terminal of the receiver has the designated operating system and the transmission module corresponding to the designated operating system. At this point, a transmission channel is established between the two transmission modules, thereby ensuring security of transmission of the data.

[0045] Specifically, data transmission can be directly performed between the designated operating system for example the secure operating system and a designated operating system of the other terminal, for example, data is directly transmitted from a secure operating system of a terminal A to a secure operating system of a terminal B.

[0046] Furthermore, for ensuring security of the data of the terminal, the secure operating system may not be allowed to directly communicate with external devices to perform data service. At this point, when data transmission is performed, the data of the secure operating system can be transmitted to the other normal operating system of the terminal, and the data is then transmitted from the other normal operating system of the terminal to a normal operating system of an external target terminal, and then the data is transmitted from the normal operating system to a designated operating system, that is, a secure operating system.

[0047] For further ensuring security of the data, encryption processing can be performed on transmission of the data. After the target terminal of the receiver receives the data, decryption processing is performed.

[0048] In the above technical solution, preferably, the designated operating system is the operating system of the multiple operating systems having the highest security level.

[0049] In the technical solution, the operating system having the highest security level, that is, the secure operating system is set to be the designated operating system, thus the security of data transmission and data storage can be ensured.

[0050] FIG. 2 is a block diagram of a data transmission device in accordance with an embodiment of the present disclosure.

[0051] As illustrated by FIG. 2, a data transmission device 200 in accordance with an embodiment of the

present includes a determining unit 202 configured to determine a target transmission mode for data of a terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode includes a normal transmission mode and a secure transmission mode. The device 200 further includes a connection establishing unit 204 configured to switch from the current operating system of the terminal to a designated operating system of multiple operating systems when the target transmission mode is the secure transmission mode, and establish a connection with the target terminal via the designated operating system, a judging unit 206 configured to determine whether the target terminal supports secure transmission, and a transmitting unit 208 configured to transmit the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission.

[0052] In the technical solution, when a user of the terminal wants the data to be securely transmitted, the secure transmission mode can be selected. When the terminal detects that the transmission mode for the data is the secure transmission, and the current operating system is not the designated operating system, the user is prompted to switch to the designated operating system or the terminal automatically switches to the designated operating system. Specifically, the designated operating system can be a secure operating system. A connection with the target terminal of the receiver is then established, and whether the target terminal supports the secure transmission is determined, that is, whether the target terminal includes a secure operating system or a secure transmission module is determined. When the determination result is yes, the data is transmitted to the target terminal via the secure transmission mode, thereby ensuring data security during data transmission and after the data is transmitted to the target terminal.

[0053] In the above technical solution, preferably, the device 200 further includes a prompting unit 210 configured to prompt the user of the terminal to terminate the transmission of the data or adopt the normal transmission mode to transmit the data to the target terminal when the determination result is that the target terminal does not support the secure transmission.

[0054] In the technical solution, when the target terminal does not support the secure transmission, for ensuring security of transmission of the data, the user is prompted to terminate the transmission of the data, or to adopt the normal transmission mode to directly transmit the data.

[0055] In the above technical solution, preferably, the judging unit 206 includes a sending unit 2062 configured to send a transmission environment check command to the target terminal, so as to cause the target terminal to check whether a corresponding designated operating system is included according to the transmission environment check command, and send a support response to the terminal when the determination result is yes, and a deciding unit 2064 configured to determine whether the support response is received from the target terminal, determine that the target terminal supports the secure transmission when the determination result is yes, and determine that the target terminal does not support the secure transmission when the determination result is no.

[0056] In the technical solution, the terminal of the transmitter sends the transmission environment check command to the target terminal of the receiver, and the target terminal determines whether the target terminal includes the designated operating system according to the command, that is, whether the target terminal includes the secure operating system. The target terminal also sends the support response when the designated operating system is included, so as to inform the terminal of the transmitter that secure transmission can be performed.

[0057] In the above technical solution, preferably, the transmitting unit 208 is configured to establish a connection between a first transmission module corresponding to the designated operating system of the terminal and a second transmission module corresponding to the designated operating system of the target terminal, and transmit the data from the first transmission module to the second transmission module.

[0058] In the technical solution, when the data can be transmitted via the secure transmission mode, it indicates that the terminal of the transmitter has the designated operating system and the transmission module corresponding to the designated operating system, and the terminal of the receiver has the designated operating system and the transmission module corresponding to the designated operating system. At this point, a transmission channel is established between the two transmission modules, thereby ensuring security of transmission of the data.

[0059] Specifically, data transmission can be directly performed between the designated operating system for example the secure operating system and a designated operating system of the other terminal, for example, data is directly transmitted from a secure operating system of a terminal A to a secure operating system of a terminal B.

[0060] Furthermore, for ensuring security of the data of the terminal, the secure operating system may not be allowed to directly communicate with external devices to perform data service. At this point, when data transmission is performed, the data of the secure operating system can be transmitted to the other normal operating system of the terminal, and the data is then transmitted from the other normal operating system of the terminal to a normal operating system of an external target terminal, and then the data is transmitted from the normal operating system to a designated operating system, that is, a secure operating system.

[0061] For further ensuring security of the data, encryption processing can be performed on transmission of the data. After the target terminal of the receiver re-

ceives the data, decryption processing is performed.

[0062] In the above technical solution, preferably, the designated operating system is the operating system of the multiple operating systems having the highest security level.

[0063] In the technical solution, the operating system having the highest security level, that is, the secure operating system is set to be the designated operating system, thus the security of data transmission and data storage can be ensured.

[0064] Take a dual system terminal (Android system and secure system) for an example, the following will specifically illustrate the technical solution of the present disclosure.

[0065] As illustrate by FIG. 3, based on the dual systems, the terminal includes two transmission modules, that is, includes a transmission module 302 of the Android system and a transmission module 304 of the secure system. The terminal further includes a transmission environment check module 306 (equivalent to the judging unit) to check transmission environment of the terminal and the receiver. When a secure transmission function is needed by a user, the local transmission environment check module firstly checks whether the secure system is running. If not, the user is prompted to switch to the secure system, and a connection with a mobile phone of the receiver is established via the transmission module of the secure system.

[0066] After the connection is successfully established, the terminal transmits a transmission environment check command to the terminal of the receiver. If the terminal of the receiver does not include the secure transmission module, the terminal of the transmitter determines that this transmission is not a secure transmission, and prompts the user to terminate the transmission or switch to the normal transmission mode.

[0067] When the receiver includes the secure transmission module, the receiver receives the check command, and prompts the user that secure transmission information is received. Under the condition of receiving an allowance from the user, the terminal of the receiver starts current reception environment check. If the secure system is not running, the user is prompted to switch to the secure system.

[0068] After finishing security check of the two parties, a connection is established between the two parties based on the transmission modules of the secure systems, and data transmission starts. After transmission, switching to the system which is running before transmission is performed according to user intention.

[0069] If the user just wants to adopt the normal transmission mode of the Android system, then the secure transmission module and the environment check module both are not needed, and transmission can be started by directly starting the Android normal transmission module.

[0070] FIG. 4 is a detailed flow chart of a data transmission method in accordance with an embodiment of the present disclosure.

[0071] As illustrated by FIG. 4, a detailed process of a data transmission method in accordance with an embodiment of the present disclosure includes following steps.

[0072] Step 402, whether secure transmission is started is determined. When the determination result is yes, step 404 is executed, and when the determination result is no, step 406 is executed.

[0073] Step 404, whether the terminal runs a secure system is determined. When the determination result is yes, step 408 is executed, and when the determination result is no, step 410 is executed.

[0074] Step 406, the transmission module 302 of the Android system is invoked to start transmission process.

[0075] Step 408, whether the terminal of the receiver runs the secure system is determined. When the determination result is yes, step 412 is executed, and when the determination result is no, step 414 is executed.

[0076] Step 410, the terminal switches to the secure system.

[0077] Step 412, the transmission module 304 of the secure system is invoked to start transmission process.

[0078] Step 414, the terminal switches to the secure system.

[0079] The above descriptions specifically illustrate the technical solution of the present disclosure in combination with the accompanying drawings. By means of the technical solution of the present disclosure, secure transmission and storage of user secure data can be ensured, and malicious attacks from other operating systems can be avoided.

[0080] The foregoing descriptions are merely preferred embodiments of the present disclosure, but are not intended to limit the present disclosure. For those skilled in the art, various changes and variations can be made according to the present disclosure. Any modifications, equivalent replacements, and improvements within the spirit and principle of the technical solution shall fall within the protection scope of the present disclosure.

Claims

1. A data transmission method applied in a terminal, the terminal comprising multiple operating systems, each operating system corresponding to a transmission module, the method comprising:

   determining a target transmission mode for data of the terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode comprises a normal transmission mode and a secure transmission mode;
   switching from the current operating system of the terminal to a designated operating system of the multiple operating systems when the target transmission mode is the secure transmission mode, and establishing a connection with

the target terminal via the designated operating system;
determining whether the target terminal supports secure transmission; and
transmitting the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission.

2. The data transmission method of claim 1, wherein the method further comprises:

prompting a user of the terminal to terminate the transmission of the data or adopt the normal transmission mode to transmit the data to the target terminal when the determination result is that the target terminal does not support the secure transmission.

3. The data transmission method of claim 1, wherein determining whether the target terminal supports the secure transmission comprises:

sending a transmission environment check command to the target terminal, so as to cause the target terminal to check whether a corresponding designated operating system is comprised according to the transmission environment check command, and send a support response to the terminal when the determination result is yes; and
determining whether the support response is received from the target terminal, determining that the target terminal supports the secure transmission when the determination result is yes, and determining that the target terminal does not support the secure transmission when the determination result is no.

4. The data transmission method of claim 3, wherein transmitting the data to the target terminal via the secure transmission mode comprises:

establishing a connection between a first transmission module corresponding to the designated operating system of the terminal and a second transmission module corresponding to the designated operating system of the target terminal, and transmitting the data from the first transmission module to the second transmission module.

5. The data transmission method of any of claims 1-4, wherein the designated operating system is the operating system of the multiple operating systems having the highest security level.

6. A data transmission device applied in a terminal, the terminal comprising multiple operating systems, each operating system corresponding to a transmission module, the data transmission device comprising:

a determining unit configured to determine a target transmission mode for data of the terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode comprises a normal transmission mode and a secure transmission mode;
a connection establishing unit configured to switch from the current operating system of the terminal to a designated operating system of the multiple operating systems when the target transmission mode is the secure transmission mode, and establish a connection with the target terminal via the designated operating system;
a judging unit configured to determine whether the target terminal supports secure transmission; and
a transmitting unit configured to transmit the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission.

7. The data transmission device of claim 6, wherein the data transmission device further comprises:

a prompting unit configured to prompt a user of the terminal to terminate the transmission of the data or adopt the normal transmission mode to transmit the data to the target terminal when the determination result is that the target terminal does not support the secure transmission.

8. The data transmission device of claim 6, wherein the judging unit comprises:

a sending unit configured to send a transmission environment check command to the target terminal, so as to cause the target terminal to check whether a corresponding designated operating system is comprised according to the transmission environment check command, and send a support response to the terminal when the determination result is yes; and
a deciding unit configured to determine whether the support response is received from the target terminal, determine that the target terminal supports the secure transmission when the determination result is yes, and determine that the target terminal does not support the secure transmission when the determination result is no.

9. The data transmission device of claim 8, wherein the transmitting unit is configured to establish a connection between a first transmission module corresponding to the designated operating system of the terminal and a second transmission module corresponding to the designated operating system of the target terminal, and transmit the data from the first transmission module to the second transmission module.

10. The data transmission device of any of claims 6-9, wherein the designated operating system is the operating system of the multiple operating systems having the highest security level.

11. A data transmission system comprising the data transmission device of any of claims 6-10.

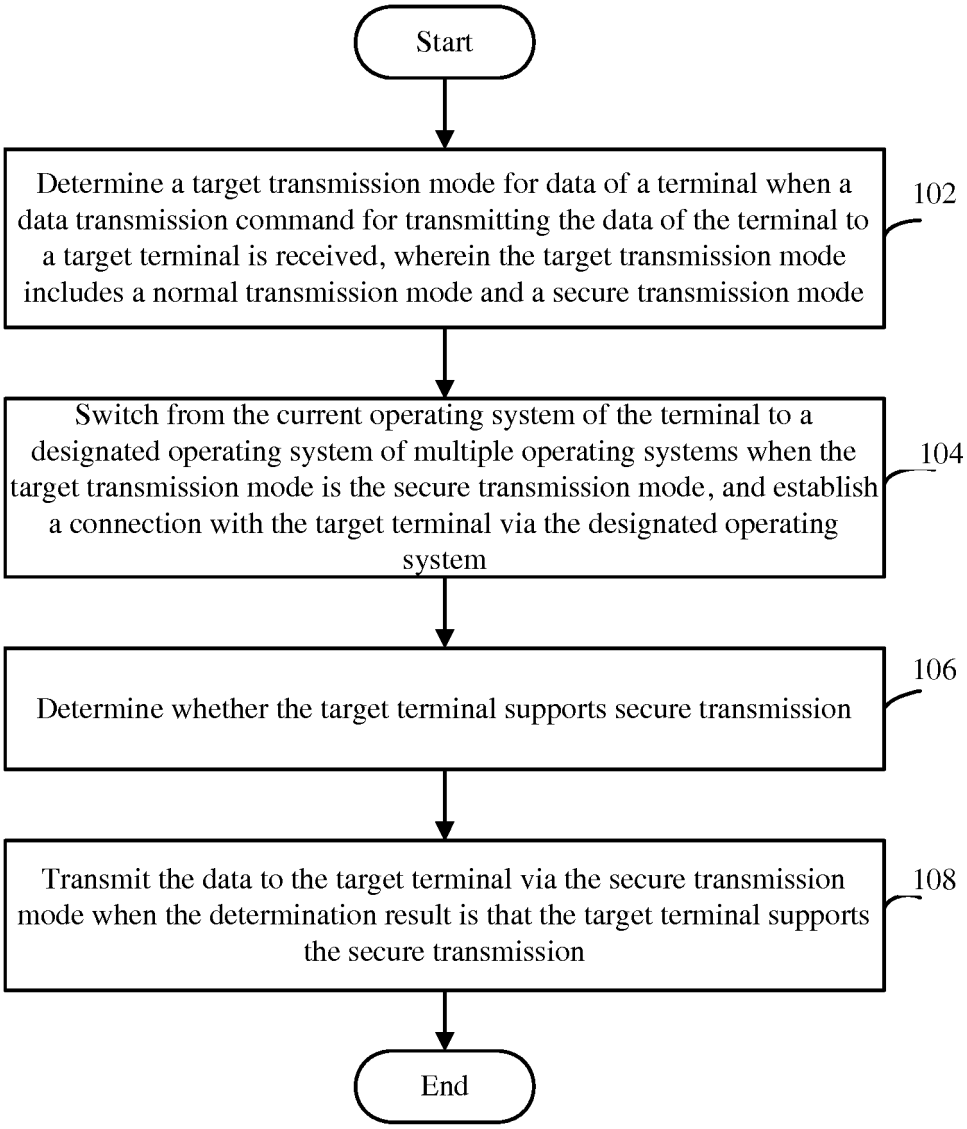
Start
Determine a target transmission mode for data of a terminal when a data transmission command for transmitting the data of the terminal to a target terminal is received, wherein the target transmission mode includes a normal transmission mode and a secure transmission mode
102
Switch from the current operating system of the terminal to a designated operating system of multiple operating systems when the target transmission mode is the secure transmission mode, and establish a connection with the target terminal via the designated operating system
104
Determine whether the target terminal supports secure transmission
106
Transmit the data to the target terminal via the secure transmission mode when the determination result is that the target terminal supports the secure transmission
108
End

FIG. 1

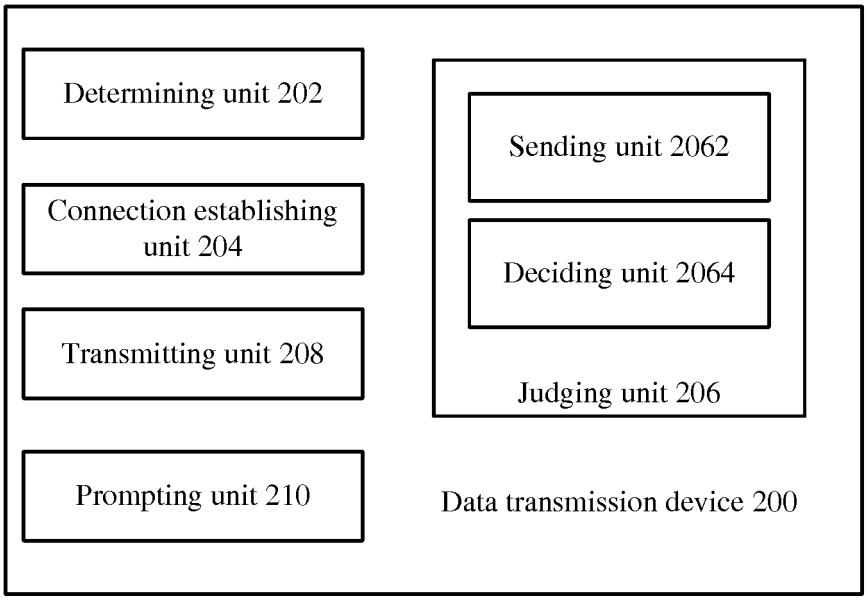
Determining unit 202
Connection establishing unit 204
Transmitting unit 208
Prompting unit 210
Sending unit 2062
Deciding unit 2064
Judging unit 206
Data transmission device 200

FIG. 2

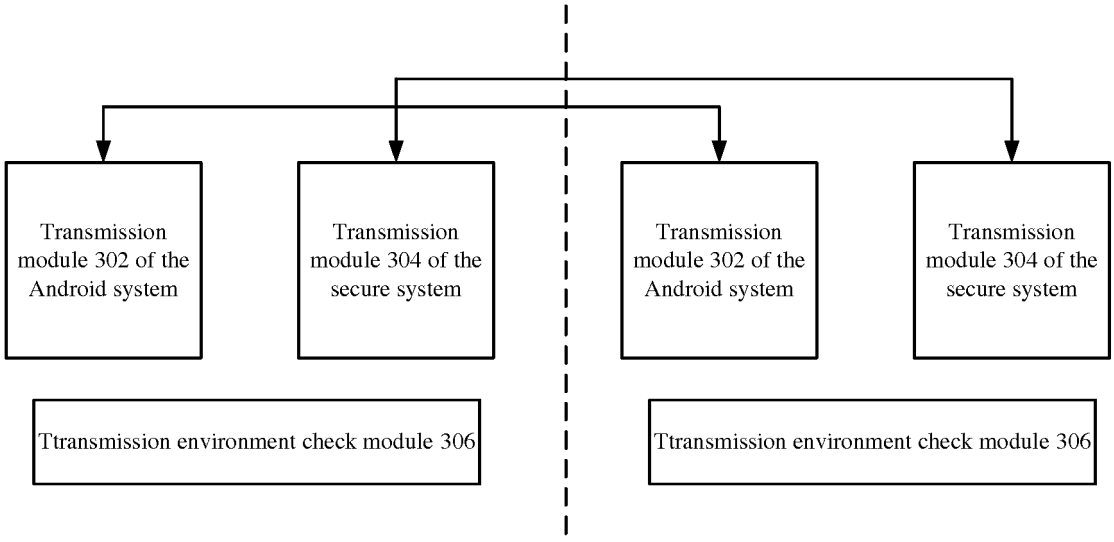
Transmission module 302 of the Android system
Transmission module 304 of the secure system
Transmission module 302 of the Android system
Transmission module 304 of the secure system
Ttransmission environment check module 306
Ttransmission environment check module 306

FIG. 3

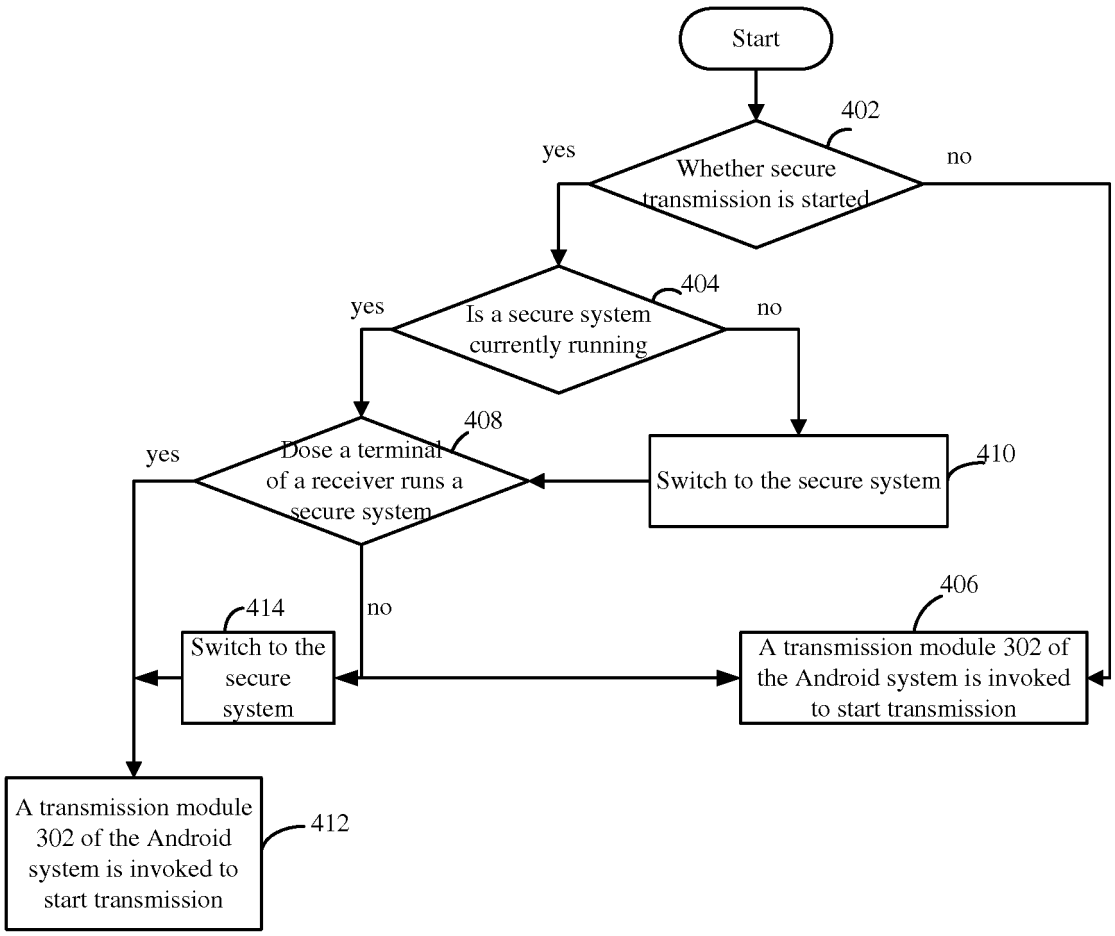
Start
402
Whether secure transmission is started
yes
no
404
Is a secure system currently running
yes
no
408
Dose a terminal of a receiver runs a secure system
yes
Switch to the secure system
410
406
A transmission module 302 of the Android system is invoked to start transmission
414
Switch to the secure system
no
A transmission module 302 of the Android system is invoked to start transmission
412

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/090092

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, VEN, CNTXT, CNKI: transfer, mode, data, support, operating system, OS, terminal, switch, safety, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102202075 A (LENOVO (BEIJING) CO., LTD.), 28 September 2011 (28.09.2011), description, paragraphs [0048]-[0105], and figures 1-3	1-11
A	CN 103618736 A (CHENGDU DAXINTONG COMMUNICATION EQUIPMENT CO., LTD.), 05 March 2014 (05.03.2014), the whole document	1-11
A	US 2013191457 A1 (IBM), 25 July 2013 (25.07.2013), the whole document	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 June 2015 (05.06.2015)	**19 June 2015 (19.06.2015)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **BIAN, Xiaofei** Telephone No.: (86-10) **62411330**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/090092

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102202075 A	28 September 2011	US 2013018977 A1	17 January 2013
		CN 102202075 B	04 December 2013
		WO 2011116626 A1	29 September 2011
CN 103618736 A	05 March 2014	None	
US 2013191457 A1	25 July 2013	GB 2498724 A	31 July 2013
		GB 201201132 D0	07 March 2012

Form PCT/ISA/210 (patent family annex) (July 2009)